CLAIMS

1. A system for detecting intrusions on a host, comprising:

an analysis engine; and

a configuration discovery mechanism, in communication with the analysis engine, for locating system files on the host.

2. The system as recited in claim 1, wherein the system files include user login files.

3. The system as recited in claim 2, wherein the system files include at least one of utmp, wtmp, lastlog, syslog, sulog, cron, and at.

4. The system as recited in claim 2, wherein the configuration discovery mechanism comprises a sensor for extracting system file locations from a system configuration file.

5. The system as recited in claim 4, wherein the system configuration file is syslog.conf.

6. The system as recited in claim 4, wherein the configuration discovery mechanism is located on a second host apart from the host.

7. An intrusion detection system, comprising:

a directory scanner for collecting directory information from a host;

a plurality of sensors configured to collect primary, secondary, and indirect information; and

an analysis engine configured to analyze the information collected by the plurality of sensors.

8. The intrusion detection system as recited in claim 7, wherein the directory scanner is further configured to collect i-node information from the host.

9. The intrusion detection system as recited in claim 8, wherein the analysis engine is configured to determine a login session for a user account, wherein the primary information includes wtmp, and wherein the secondary information includes access times of files related to a shell associated with the user account.

10. The intrusion detection system as recited in claim 9, wherein the indirect information includes logfiles other than wtmp.

11. The intrusion detection system as recited in claim 10, wherein the indirect information includes sulog.

12. The intrusion detection system as recited in claim 9, wherein the indirect information includes timestamps on directories and files accessible only by the user account.

13. The intrusion detection system as recited in claim 8, wherein the analysis engine is configured to examine logfiles for null-bytes.

14. An intrusion detection system, comprising:

a directory scanner for collecting directory information from a host; and

an analysis engine coupled to the directory scanner and configured to identify logfiles that are being rolled down.

15. The intrusion detection system as recited in claim 14, wherein the analysis engine is further configured to determine a scheme being used in rolling down the logfiles.

16. The intrusion detection system as recited in claim 15, further comprising a sensor configured to collect information from the logfiles, and wherein the analysis engine is configured to invoke the sensor with a specification of a sequence of logfiles to collect.

17. The intrusion detection system as recited in claim 14, wherein the sensor is further configured to determine a year of an entry in the logfiles.

18. The intrusion detection system as recited in claim 17, wherein the logfiles include syslog.

19. A system for detecting intrusions on a host, comprising:

a sensor for collecting information from a logfile located on the host; and

an analysis engine coupled to the sensor for analyzing the logfile and including a time decay function.

20. The intrusion detection system as recited in claim 19, wherein the analysis engine is configured to use the time decay function in computing a suspicion value for an entry in the logfile.

21. The intrusion detection system as recited in claim 20, wherein the analysis engine is configured to use the time decay function to compute a probability for an end of a session.

22. The intrusion detection system as recited in claim 21, wherein the logfile is sulog and the session is an su session.

23. A method for detecting intrusions on a host, comprising the steps of:

providing an analysis engine; and

discovering locations of system files on the host.

24. A computer program product for detecting intrusions on a host, the computer program product being embodied in a computer readable medium having machine readable code embodied therein for performing the steps of:

providing an analysis engine; and

discovering locations of system files on the host.